The listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims

1. Cancelled.

2. (Currently Amended) A method of controlling updates of a programmable memory of a device, the method comprising:

providing an update window of predefined duration during which the programmable memory may be updated; and

allowing updates of the programmable memory only during the update window;

wherein the steps of providing an update window and allowing updates comprise the steps of:

allowing access to the programmable memory based on the state of an access latch;

setting the access latch to allow access to the programmable memory after a hardware reset of the device;

executing an update control program to control access to the programmable memory; ~~and~~

resetting the latch to prevent access to the programmable memory upon completion of the update control program; .

allowing access to a memory where the update control program resides when the access latch allows access to the programmable memory; and

preventing access to the memory where the update control program resides when the access latch prevents access to the programmable memory.

3. Cancelled.

4. (Original) A method according to Claim 2, wherein the update control program further carries out the steps of:

determining if an update of the programmable memory is available; and

updating the programmable memory if an update of the programmable memory is available.

5. (Original) A method according to Claim 4, wherein the step of determining if an update of the programmable memory is available comprises examining at least one of a local memory location, a local drive, a network drive and an input device status to determine if an update is available.

6. (Original) A method according to Claim 4, wherein the step of determining if an update of the programmable memory is available comprises examining persistent status information.

7. (Original) A method according to Claim 4, wherein the step of updating the programmable memory comprises the steps of:

obtaining an update image associated with the available update containing update data to be written to the programmable memory;

obtaining installation information from the update image; and

writing the update data to the programmable memory based on the installation information obtained from the update image.

8. (Original) A method according to Claim 7, wherein the installation information comprises an install program and wherein the step of writing the update data to the programmable memory based on the installation information obtained from the update image comprises executing the install program to write the update data to the programmable memory.

9. (Original) A method according to Claim 4, wherein the step of updating the programmable memory comprises the steps of:

loading an update image associated with the available update into a temporary workspace; and

updating the programmable memory from the loaded update image.

10. (Original) A method according to Claim 4, further comprising the step of storing existing data from the programmable memory so as to provide a backup copy of the existing data from the programmable memory.

11. (Original) A method according to Claim 10, further comprising the steps of:

determining if the update of the programmable memory was successful; and

restoring the contents of the programmable memory from the backup copy if the update of the programmable memory was not successful.

12. (Original) A method according to Claim 4, wherein the update control program further carries out the step of:

verifying the authenticity of the update of the programmable memory if an update of the programmable memory is available.

13. (Original) A method according to Claim 12, wherein the step of verifying the authenticity of the update comprises the step of:

evaluating at least one certificate in an update image associated with the available update to determine if a valid digital signature is provided with the update image.

14. (Original) A method according to Claim 12, wherein the step or verifying the authenticity of the update comprises the step of determining if a valid digital signature is provided with the image by decrypting the digital signature provided with the image using a shared secret.

15. (Original) A method according to Claim 13, wherein the step of evaluating at least one certificate comprises the steps of:

decrypting a digital signature of the certificate utilizing a public key of a certificate authority accessible to the update program; and

comparing the decrypted digital signature with a precomputed value to determine if the digital signature is a valid digital signature associated with the certificate authority.

16. (Original) A method according to Claim 15, wherein the public key is stored in a non-updateable memory associated with the update control program.

17. (Original) A method according to Claim 15, further comprising the step of:

providing the public key of the certificate authority in a previous version of data to be stored in the programmable memory; and

wherein the step of decrypting a digital signature of the certificate utilizing a public key further comprises the step of obtaining the public key from the programmable memory.

18. (Original) A method according to Claim 12, wherein the update includes a plurality of certificates in a hierarchy of certificates and wherein the step of verifying the authenticity of the update comprises the step of evaluating certificates of the plurality of certificates in an update image to determine if a valid digital signature is provided with certificates of the plurality of certificates in the update image.

19. (Original) A method according to Claim 18, wherein the step of evaluating certificates of the plurality of certificates comprises the steps of:

decrypting a digital signature of a certificate utilizing a public key associated with a next-higher certificate in the hierarchy;

comparing the decrypted digital signature with a precomputed value to determine if the digital signature is a valid digital signature associated with the certificate;

obtaining a public key associated with another of the digital certificates;

repeating the steps of decrypting and comparing utilizing the obtained public key associated with another of the digital certificates; and

wherein the step of obtaining a public key is repeated until a public key associated with a last of the digital certificates is obtained, and comparing the last public key with a predetermined value.

20. (Original) A method according to Claim 12, further comprising the steps of:

obtaining application rules information from an extension of at least one certificate associated with the update;

evaluating the rules information obtained from the at least one certificate; and

wherein the step of updating the programmable memory comprises the step of selectively updating the programmable memory based on the evaluation of the rules information obtained from the at least one certificate.

21. (Previously Presented) A method according to Claim 20, wherein the step of evaluating the rules information comprises the step of evaluating at least one of rules information associated with a manufacturer of the device, rules information associated with a brand of the device, rules information associated with a software version of the device, rules information associated with a license authorization of the device or rules information associated with the individual device.

22.-39. Cancelled.

40. (Currently Amended) A system for controlling updates of a programmable memory of a device, comprising:

means for providing an update window of predefined duration during which the programmable memory may be updated; and

means for allowing updates of the programmable memory only during the update window;

wherein the means for providing an update window and the means for allowing updates, comprise:

means for allowing access to the programmable memory based on the state of an access latch;

means for setting the access latch to allow access to the programmable memory after a hardware reset of the device;

means for executing an update control program to control access to the programmable memory; ~~and~~

means for resetting the latch to prevent access to the programmable memory upon completion of the update control program;

means for allowing access to a memory where the update control program resides when the access latch allows access to the programmable memory; and

means for preventing access to the memory where the update control program resides when the access latch prevents access to the programmable memory.

41. Cancelled.

42. (Original) A system according to Claim 40, further comprising:

means for determining if an update of the programmable memory is available; and

means for updating the programmable memory if an update of the programmable memory is available.

43. (Original) A system according to Claim 42, wherein the means for determining if an update of the programmable memory is available comprises means for examining at least one of a local memory location, a local drive, a network drive and an input device status to determine if an update is available.

44. (Original) A system according to Claim 42, wherein the means for determining if an update of the programmable memory is available comprises means for examining persistent status information.

45. (Original) A system according to Claim 42, wherein the means for updating the programmable memory comprises:

means for obtaining an update image associated with the available update containing update data to be written to the programmable memory;

means for obtaining installation information from the update image; and

means for writing the update data to the programmable memory based on the installation information obtained from the update image.

46. (Original) A system according to Claim 45, wherein the installation information comprises an install program and wherein the means for writing the update data to the programmable memory based on the installation information obtained from the update image comprises means for executing the install program to write the update data to the programmable memory.

47. (Original) A system according to Claim 40, wherein the means for updating the programmable memory comprises:

means for loading an update image associated with the available update into a temporary workspace; and

means for updating the programmable memory from the loaded update image.

48. (Original) A system according to Claim 40, further comprising means for storing existing data from the programmable memory so as to provide a backup copy of the existing data from the programmable memory.

49. (Original) A system according to Claim 48, further comprising:

means for determining if the update of the programmable memory was successful; and

means for restoring the contents of the programmable memory from the backup copy if the update of the programmable memory was not successful.

50. (Original) A system according to Claim 40, further comprising means for verifying the authenticity of the update of the programmable memory if an update of the programmable memory is available.

51. (Original) A system according to Claim 50, wherein the means for verifying the authenticity of the update comprises means for evaluating at least one certificate

in update image associated with the available update to determine if a valid digital signature is provided with the update image.

52. (Original) A system according to Claim 50, wherein the means for verifying the authenticity of the update image comprises means for determining if a valid digital signature is provided with the image by decrypting the digital signature provided with the image using a shared secret.

53. (Original) A system according to Claim 51, wherein the means for evaluating at least one certificate comprises:

means for decrypting a digital signature of the certificate utilizing a public key of a certificate authority accessible to the update program; and

means for comparing the decrypted digital signature with a precomputed value to determine if the digital signature is a valid digital signature associated with the certificate authority.

54. (Original) A system according to Claim 53, wherein the public key is stored in a non-updateable memory associated with the update control program.

55. (Original) A system according to Claim 53, further comprising:

means for providing the public key of the certificate authority in a previous version of data to be stored in the programmable memory; and

wherein means for decrypting a digital signature of the certificate utilizing a public key further comprises means for obtaining the public key from the programmable memory.

56. (Original) A system according to Claim 51, further comprising:

means for obtaining application rules information from an extension of at least one certificate associated with the update;

means for evaluating the rules information obtained from the at least one certificate; and

wherein the means for updating the programmable memory comprises means for selectively updating the programmable memory based on the evaluation of the rules information obtained from the at least one certificate.

57. (Original) A system according to Claim 56, wherein the means for evaluating the rules information comprises means for evaluating at least one of rules information associated with a manufacturer of the device, rules information associated with a brand of the device, rules information associated with a software version of the device, rules information associated with a license authorization of the device or rules information associated with the individual device.

58.-79. Cancelled.